

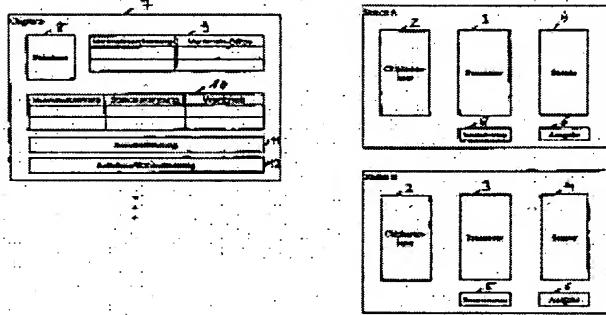
Data carrier such as chip-card, for biometric user-authentication has two different sets of biometric characteristics stored in carrier and associated with different stations

Patent number: DE10206843
Publication date: 2003-09-04
Inventor: KAPPE FRANK (DE); RUEBBELKE HERMANN (DE); DANIEL THORSTEN (DE)
Applicant: ORGA KARTENSYSTEME GMBH (DE)
Classification:
- **international:** G06K19/10
- **european:** G06K19/10; G07C9/00B6D4
Application number: DE20021006843 20020218
Priority number(s): DE20021006843 20020218

[Report a data error here](#)

Abstract of DE10206843

The data carrier (7) stores two different sets (9,10) of biometric characteristics that belong to the same user, and relate to the same biometric characteristic. Each set is associated with one or more stations (1). The data carrier may include a device for receiving a station ID, and a processor (8) for selecting a set of characteristics according to the station ID. Independent claims are also included for: (1) a station for biometric user-authentication; (2) a method of biometric user-authentication; and (3) a computer program product for carrying out the method.



Data supplied from the esp@cenet database - Worldwide

THIS PAGE BLANK (USPTO)

⑯ BUNDESREPUBLIK

DEUTSCHLAND



DEUTSCHES
PATENT- UND
MARKENAMT

⑯ Offenlegungsschrift
⑯ DE 102 06 843 A 1

51 Int. Cl. 7:
G 06 K 19/10

M203-ZP

⑯ Aktenzeichen: 102 06 843.7
⑯ Anmeldetag: 18. 2. 2002
⑯ Offenlegungstag: 4. 9. 2003

⑯ Anmelder:
ORGAN Kartensysteme GmbH, 33104 Paderborn, DE
⑯ Vertreter:
Quermann & Richard Patentanwälte, 65195 Wiesbaden

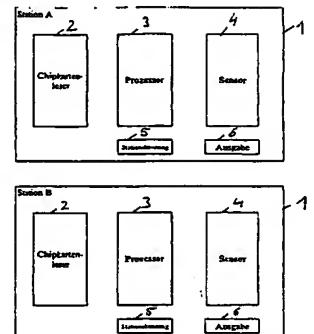
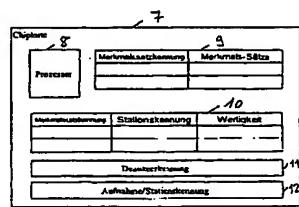
⑯ Erfinder:
Kappe, Frank, 33378 Rheda-Wiedenbrück, DE;
Rübelke, Hermann, 33129 Delbrück, DE; Daniel,
Thorsten, 33102 Paderborn, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

⑯ Datenträger, Station und Verfahren für die biometrische Benutzer-Authentisierung

⑯ Die Erfindung betrifft eine Chipkarte für die biometrische Benutzer-Authentisierung mit zumindest einem ersten biometrischen Merkmals-Satz und einem zweiten biometrischen Merkmals-Satz, wobei die ersten und zweiten biometrischen Merkmals-Sätze voneinander verschieden sind, zu dem selben Benutzer gehören und dasselbe biometrische Merkmal betreffen.



DE 102 06 843 A 1

Beschreibung

[0001] Die Erfindung betrifft einen Datenträger, insbesondere eine Chipkarte oder einen RF ID Tag oder Token, eine Station, ein System sowie ein Verfahren und ein entsprechendes Computerprogrammprodukt für die biometrische Benutzer-Authentisierung.

[0002] Verfahren für die biometrische Benutzer-Authentisierung mit Hilfe von Chipkarten sind an sich aus dem Stand der Technik bekannt. Im Allgemeinen dient die biometrische Benutzer-Authentisierung als Schutz vor der Verwendung einer Chipkarte durch einen nicht autorisierten Benutzer. Geht etwa eine Chipkarte mit einer schützenswerten Anwendung verloren oder wird sie gestohlen, dann soll sie von einem unrechtmäßigen Benutzer nicht verwendet werden können. Dies wird durch die biometrische Benutzer-Authentisierung sichergestellt. Einen Überblick über entsprechende Verfahren gibt Bruno Struif, "Wissensbasirte und basierte Benutzer-Authentisierung", Card-Forum 11/97.

[0003] Aus der DE 198 45 300 A1 ist ein Verfahren zum Freigeben einer Benutzungsberechtigung, insbesondere für ein Kraftfahrzeug, basierend auf einer Chipkarte mit biometrischen Daten und fahrzeugspezifischen Daten bekannt. Die Berechtigung zur Fahrzeugbenutzung wird erst freigegeben, wenn ein Vergleich der auf der Chipkarte gespeicherten Daten mit von einer fahrzeugfesten Biometriesensorvorrichtung erfassten biometrischen Daten und mit im Fahrzeug gespeicherten fahrzeugspezifischen Daten positiv ist.

[0004] Aus US 6,128,398 ist ein auf Chipkarten basierendes biometrisches Verfahren mittels der Prüfung von Gesichts-Merkmalen bekannt. Hierzu wird eine Abbildung des Gesichts auf der Chipkarte gespeichert.

[0005] Aus EP 0 786 735 A2 ist ein Verfahren zur Erzeugung eines biometrischen Merkmals-Satzes für einen Fingerabdruck bekannt. Für die Verifikation eines durch einen Fingerabdruck-Sensor erfassten Fingerabdrucks wird auf eine Datenbank zugegriffen, in der für jeden Benutzer ein Fingerabdruck gespeichert ist.

[0006] Aus der EP 0 372 762 B1 ist ein weiteres Verfahren zum Identifizieren eines Fingerabdrucks bekannt. Die Identifikation erfolgt durch Vergleich eines Referenz-Merkmals-Satzes des Fingerabdrucks, der für eine bekannte Person registriert worden ist, mit dem Merkmals-Satz eines Fingerabdruckbildes, welches zu identifizieren ist.

[0007] Aus dem Stand der Technik sind darüber hinaus weitere Verfahren für die biometrische Benutzer-Authentisierung basierend auf anderen biometrischen Merkmalen, wie beispielsweise die Merkmale der Iris eines Benutzers, bekannt.

[0008] Der Erfindung liegt die Aufgabe zu Grunde einen verbesserten Datenträger, eine verbesserte Station und ein entsprechendes System für die biometrische Benutzer-Authentisierung zu schaffen. Der Erfindung liegt ferner die Aufgabe zu Grunde ein verbessertes Verfahren für die biometrische Benutzer-Authentisierung und ein entsprechendes Computerprogrammprodukt zu schaffen.

[0009] Die der Erfindung zu Grunde liegende Aufgabe wird jeweils mit den Merkmalen der unabhängigen Patentansprüche gelöst. Bevorzugte Ausführungsformen der Erfindung sind in den abhängigen Patentansprüchen angegeben.

[0010] Die vorliegende Erfindung ermöglicht es für ein und dasselbe biometrische Merkmal eines Benutzers zumindest zwei verschiedene Merkmals-Sätze für die biometrische Benutzer-Authentisierung zu verwenden. Dies hat den Vorteil, dass eine biometrische Benutzer-Authentisierung mittels eines vorgegebenen biometrischen Authentisierungsverfahrens in verschiedenen Umgebungen und unter

verschiedenen Bedingungen sicher durchgeführt werden kann.

[0011] Nach einer bevorzugten Ausführungsform der Erfindung wird mittels eines Sensors ein biometrisches Merkmal des zu authentisierenden Benutzers aufgenommen. Aufgrund dieser Aufnahme wird ein biometrischer Verifikations-Datensatz generiert, der zum Vergleich mit zuvor aufgenommenen biometrischen Referenz-Merkmales-Sätzen dient.

[0012] Die Aufnahme des biometrischen Merkmals wird typischerweise durch die Umgebung beeinflusst, in der sich der biometrische Sensor befindet. Beispielsweise wird die Aufnahme von den jeweiligen Beleuchtungsverhältnissen beeinflusst. Ein weiterer Einfluss ist das aktuelle Erscheinungsbild des Benutzers; dieses kann aufgrund einer geänderten Frisur, Brille, Bart, Sonnenbräune etc. variieren. Entsprechend variieren auch die aus solchen Aufnahmen generierten biometrischen Merkmals-Sätze in Abhängigkeit von den Umgebungsbedingungen und/oder dem aktuelle Erscheinungsbild des Benutzers.

[0013] Neben der Beeinflussung durch die Umgebung kann die Aufnahme auch durch den Sensor selbst beeinflusst werden. Beispielsweise kann sich eine solche Beeinflussung aus einer Alterung des Sensors ergeben oder aus unterschiedlichen Sensortypen mit unterschiedlichen Auflösungen, die an verschiedenen Stationen eingesetzt werden.

[0014] Die Erfindung ist von besonderem Vorteil, da mehrere biometrische Referenz-Merkmales-Sätze verwendet werden, die z. B. auf unterschiedliche Umgebungen, wie zum Beispiel Beleuchtungssituationen, abgestimmt sind. So wird etwa für den Fall der biometrischen Benutzer-Authentisierung basierend auf Gesichtsmerkmalen je eine Aufnahme bei unterschiedlichen Beleuchtungsverhältnissen gemacht und hieraus entsprechende Merkmals-Sätze generiert. Darüber hinaus können auch verschiedene Merkmalsätze z. B. mit und ohne Brille aufgenommen werden.

[0015] Für die biometrische Benutzer-Authentisierung können die verschiedenen Referenz-Merkmales-Sätze mit dem Verifikations-Merkmales-Satz verglichen werden. Wenn mindestens einer der Referenz-Merkmales-Sätze eine hinreichende Übereinstimmung mit dem Verifikations-Merkmales-Satz aufweist, so gilt der Benutzer als authentisiert.

[0016] Dies ist besonders für räumlich verteilte Zugangskontrollsysteme vorteilhaft. Erfindungsgemäß können solche Zugangskontrollsysteme verschiedene Stationen für die Zugangskontrolle aufweisen, die geographisch verteilt sind und sich in unterschiedlichen Umgebungen befinden. Beispielsweise können Stationen des Zugangskontrollsysteins unter freiem Himmel und andere innerhalb von Gebäuden angeordnet sein, wobei die Beleuchtungsverhältnisse entsprechend variieren. Die Erfindung erlaubt trotz dieser unterschiedlichen Umgebungsbedingungen eine sichere biometrische Benutzer-Authentisierung aufgrund verschiedener Merkmals-Sätze, die auf solche unterschiedlichen Umgebungsbedingungen abgestimmt sind. Auch wenn für unterschiedliche Stationen verschiedene Sensortypen zum Beispiel mit verschiedenen Auflösungen verwendet werden, erlaubt die Erfindung eine sichere Benutzer-Authentisierung aufgrund der Verwendung verschiedener Merkmals-Sätze.

[0017] Nach einer bevorzugten Ausführungsform der Erfindung werden verschiedene biometrische Referenz-Merkmales-Sätze auf einer Chipkarte abgespeichert. Jedem dieser Merkmals-Sätze wird je eine oder mehrere Stationen eines Zugangskontrollsysteins zugeordnet. Dies kann so erfolgen, dass jeder Station eine eindeutige Stationskennung zugeordnet ist.

[0018] Auf der Karte wird dann eine Datei gespeichert, die jedem Merkmals-Satz ein oder mehrere der Stationen

zuordnet. Für die Durchführung einer Benutzer-Authentisierung wird die Chipkarte in ein Chipkarten-Lesegerät der Station eingeführt. Dann wird entweder seitens der Station oder seitens der Chipkarte basierend auf der Stationskennung ein Referenz-Merkmals-Satz ausgewählt, der für den Vergleich mit dem Verifikations-Merkmals-Satz verwendet wird.

[0019] Nach einer weiteren bevorzugten Ausführungsform der Erfindung können jedem Referenz-Merkmals-Satz auch mehrere Stationen zugeordnet sein. Die Zuordnung einer Station zu einem Merkmals-Satz ist dann mit einer Wertigkeit versehen, die eine Aussage betreffend der Verifikationsgüte beinhaltet. Als Verifikationsgüte wird dabei das Maß der Übereinstimmung zwischen dem betreffenden Referenz-Merkmals-Satz und einem Verifikations-Merkmals-Satz, der an der betreffenden Station aufgenommen worden ist, bezeichnet.

[0020] Wenn mehrere Merkmals-Sätze zur Verfügung stehen, die derselben Station zugeordnet sind, an der eine Benutzer-Authentisierung vorzunehmen ist, wird derjenige Referenz-Merkmals-Satz gewählt, der die höchste Wertigkeit aufweist. Zusätzlich können noch weitere Referenz-Merkmals-Sätze ausgewählt werden, die ebenfalls dieser Station zugeordnet sind, aber geringere Wertigkeiten aufweisen. Diese ausgewählten Referenz-Merkmals-Sätze werden dann mit dem Verifikations-Merkmals-Satz verglichen; wenn zumindest einer der Referenz-Merkmals-Sätze hinreichend mit dem Verifikations-Merkmals-Satz übereinstimmt, gilt der betreffende Benutzer als authentisiert.

[0021] Nach einer weiteren bevorzugten Ausführungsform der Erfindung wird von der Chipkarte eine Datei mit Merkmals-Satz-Kennungen und den Merkmals-Satz-Kennungen zugeordneten Stationskennungen und Wertigkeiten übertragen. Aufgrund dieser Datei erfolgt dann stationsseitig eine Auswahl der Referenz-Merkmals-Sätze. Die ausgewählten Referenz-Merkmals-Sätze werden dann mittels deren Merkmals-Satz-Kennung von der Chipkarte durch die Station angefordert und von der Chipkarte an die Station übertragen. Durch die Station wird dann auch der Vergleich mit dem Verifikations-Merkmals-Satz vorgenommen.

[0022] Nach einer weiteren bevorzugten Ausführungsform der Erfindung wird von der Station die Stationskennung an die Chipkarte übertragen. Basierend auf der Stationskennung erfolgt dann chipkartenseitig die Auswahl eines oder mehrerer Referenz-Merkmals-Sätze. Der oder die ausgewählten Referenz-Merkmals-Sätze werden dann von der Chipkarte an die Station übertragen, die hierauf basierend den Vergleich mit dem Verifikations-Merkmals-Satz vornimmt.

[0023] Nach einer weiteren bevorzugten Ausführungsform der Erfindung wird wiederum die Stationskennung von der Station an die Chipkarte übertragen, so dass die Chipkarte basierend auf der Stationskennung ein oder mehrere Referenz-Merkmals-Sätze auswählt. Ferner wird auch der Verifikations-Merkmals-Satz von der Station zu der Chipkarte übertragen. Der Vergleich zwischen dem oder den Referenz-Merkmals-Sätzen mit dem Verifikations-Merkmals-Satz erfolgt dann chipkartenseitig.

[0024] Nach einer weiteren bevorzugten Ausführungsform der Erfindung ist die Wertigkeit eines Referenz-Merkmals-Satzes mit Bezug auf eine bestimmte Station adaptiv. Erfolgt beispielsweise eine Benutzer-Authentisierung aufgrund eines Referenz-Merkmals-Satzes mit einer relativ geringen Wertigkeit, so wird diese relativ geringe Wertigkeit durch eine der tatsächlich erreichten Verifikationsgüter angepassten Wertigkeit überschrieben.

[0025] Nach einer weiteren bevorzugten Ausführungsform der Erfindung wird ein Verifikations-Merkmals-Satz

als Referenz-Merkmals-Satz auf der Chipkarte gespeichert, nachdem eine Authentisierung erfolgt ist. Dies ist insbesondere dann vorteilhaft, wenn mit diesem Verifikations-Merkmals-Satz eine besonders hohe Verifikationsgüte erreicht

5 worden ist.
[0026] Nach einer weiteren bevorzugten Ausführungsform der Erfindung wird die durch die Station ermittelte Aufnahme zu der Chipkarte übertragen und dort abgespeichert, wenn eine Benutzerauthentisierung nicht erfolgen

10 konnte. Bei der Aufnahme handelt es sich um Rohdaten, zum Beispiel in Form einer Bilddatei im Fall von Gesichts-, Iris- oder Fingerabdruckerkennung oder in Form einer Tondatei im Fall von Spracherkennung oder in Form einer Videosequenz für den Fall der Lippenbewegung als biometrischem Merkmal.

[0027] Die Übertragung der Aufnahme zu der Chipkarte erfolgt also dann, wenn keine hinreichende Übereinstimmung der ausgewählten Referenz-Merkmals-Sätze mit dem Verifikations-Merkmals-Satz festgestellt werden konnte. 15 Vorzugsweise wird auch die Stationskennung der Station, welche die Aufnahme durchgeführt hat, mit zu der Chipkarte übertragen. Dies ermöglicht es einem Administrator zu einem späteren Zeitpunkt aus der Aufnahme einen Merkmalsatz zu gewinnen und ihm eine Stationskennung zuzuordnen.

[0028] Dies kann daran liegen, dass sich das biometrische Merkmal des Benutzers selbst verändert hat. Im Fall einer biometrischen Benutzer-Authentisierung basierend auf Gesichtsmerkmale kann eine solche Situation zum Beispiel eintreten, wenn sich der Benutzer einen Bart wachsen lassen hat oder wenn der Benutzer gealtert ist. Im Fall der Benutzer-Authentisierung mittels Fingerabdrucks-Verifikation kann sich das biometrische Merkmal zum Beispiel aufgrund einer Verletzung der Fingerkuppen geändert haben.

[0029] Der Benutzer hat dann die Möglichkeit sich mit seiner Chipkarte an einen Administrator zu wenden, der aufgrund der auf der Chipkarte gespeicherten Aufnahme einen neuen Referenz-Merkmals-Satz generiert und auf der Chipkarte abspeichert.

[0030] Alternativ kann statt der Aufnahme auch der von der Station selbst aufgrund der Aufnahme generierte Merkmals-Satz als neuer Referenz-Merkmals-Satz auf der Chipkarte gespeichert werden; dieser muss dann durch den Administrator freigegeben werden.

[0031] Die Erfindung ermöglicht es also ein dezentrales System für die biometrische Benutzer-Authentisierung zu schaffen. Insbesondere ist es von Vorteil, dass die verschiedenen Stationen nicht miteinander vernetzt sein müssen, und dass keine zentrale Datenhaltung der Referenz-Merkmals-Sätze erforderlich ist. Dies ist unter den Gesichtspunkten der Sicherheit zum Beispiel eines Zugangskontrollsysteins sowie unter dem Gesichtspunkt des Datenschutzes optimal.

[0032] Besonders vorteilhaft ist ferner, dass es nicht unbedingt erforderlich ist, dass die Referenz-Merkmals-Sätze von der Chipkarte an die Station für die Durchführung der Benutzer-Authentisierung übertragen werden, sondern dass die Auswahl der Referenz-Merkmals-Sätze und der Vergleich der ausgewählten Referenz-Merkmals-Sätze mit dem

60 Verifikations-Merkmals-Satz chipkartenseitig erfolgt. Dadurch ist ein besonderes Maß an Sicherheit gegeben, da auch durch Manipulation einer Station keine Möglichkeit besteht, Kopien der Referenz-Merkmals-Sätze herzustellen.

[0033] Ein weiterer besonderer Vorteil der Erfindung liegt darin, dass die Datenübertragung zwischen der Chipkarte und der Station auf ein Minimum beschränkt werden kann. Beispielsweise wird für die Auswahl von Merkmals-Sätzen nur eine Merkmals-Liste mit Stationskennungen und den

Stationskennungen zugeordneten Merkmals-Satz-Kennungen und zugehörigen Wertigkeiten übertragen, die es der Station ermöglicht eine Auswahl aus den Merkmals-Sätzen zu treffen. In diesem Fall fordert die Station mittels der Merkmals-Satz-Kennungen die ausgewählten Merkmals-Sätze an. Diese werden dann in der Reihenfolge ihrer Wertigkeit von der Chipkarte an die Station übertragen. Sobald stationsseitig eine hinreichende Übereinstimmung eines der übertragenden Merkmals-Sätze mit dem Verifikations-Merkmals-Satz festgestellt werden konnte, wird die Übertragung der weiteren ausgewählten Merkmals-Sätze von der Chipkarte an die Station abgebrochen.

[0034] Ferner kann die Auswahl der Merkmals-Sätze auch chipkartenseitig erfolgen. In diesem Fall ist das Volumen der Datenübertragung zwischen der Chipkarte und der Station weiter reduziert, da es nicht erforderlich ist, die Liste der Merkmals-Sätze von der Chipkarte an die Station zu übertragen.

[0035] Noch weiter wird das Volumen der Datenübertragung reduziert, wenn sowohl die Auswahl der Merkmals-Sätze als auch der Vergleich der ausgewählten Merkmals-Sätze mit dem Verifikations-Merkmals-Satz chipkartenseitig erfolgt. Aufgrund des relativ geringen zwischen der Chipkarte und der Station zu übertragenden Datenvolumens ist also die für die Datenübertragung erforderliche Zeit kurz, so dass die Benutzer-Authentisierung entsprechend schnell durchgeführt werden kann, was insbesondere für Zugangskontrollsystem von großem Vorteil ist.

[0036] Nach einer weiteren bevorzugten Ausführungsform der Erfindung werden die Vergleiche der ausgewählten Merkmals-Sätze mit dem Verifikations-Merkmals-Satz so durchgeführt, dass zuerst der ausgewählte Merkmals-Satz mit der höchsten Wertigkeit und danach weitere ausgewählte Merkmals-Sätze, die nach abnehmender Wertigkeit sortiert sind, mit dem Verifikations-Merkmals-Satz verglichen werden. Dadurch ist eine hohe Wahrscheinlichkeit gegeben, dass bereits zu Beginn der Vergleiche der ausgewählten Merkmals-Sätze mit dem Verifikations-Merkmals-Satz eine hinreichende Übereinstimmung festgestellt werden kann, so dass auf weitere Vergleiche verzichtet werden kann. Auch hierdurch wird die für die Benutzer-Authentisierung erforderliche Zeit minimiert.

[0037] Grundsätzlich kann die Erfindung für verschiedenste Arten von Datenträgern verwendet werden, wie zum Beispiel für sogenannte RF ID Tags oder Token oder andere Sicherheitsprodukte mit einem Speicher für biometrische Merkmals-Sätze. Insbesondere kann die Erfindung auch für berührungslos arbeitende Systeme eingesetzt werden. Besonders vorteilhaft ist die Verwendung von Chipkarten, da diese eine gegenseitige Authentisierung der Chipkarte und der Station erlauben. Hierbei kann ein sogenannter Session Key generiert werden, der die Kommunikation zwischen der Chipkarte und der Station vor unbefugtem Zugriff und Manipulationen schützt.

[0038] Im Weiteren werden bevorzugte Ausführungsbeispiele der Erfindung mit Bezugnahme auf die Zeichnungen näher erläutert. Es zeigen:

[0039] Fig. 1 ein Blockdiagramm einer Ausführungsform eines erfindungsgemäßen Systems mit mehreren Chipkarten und Stationen,

[0040] Fig. 2 eine erste Ausführungsform eines erfindungsgemäßen Verfahrens, wobei die Auswahl der Referenz-Merkmals-Sätze und die Durchführung des Vergleichs stationsseitig erfolgt,

[0041] Fig. 3 eine zweite Ausführungsform eines erfindungsgemäßen Verfahrens, wobei die Auswahl der Referenz-Merkmals-Sätze chipkartenseitig und der Vergleich stationsseitig erfolgt,

[0042] Fig. 4 eine dritte Ausführungsform eines erfindungsgemäßen Verfahrens, wobei sowohl die Auswahl der Referenz-Merkmals-Sätze als auch der Vergleich chipkartenseitig erfolgt.

[0043] Die Fig. 1 zeigt ein Blockdiagramm eines Zugangskontrollsystems. Das Zugangskontrollsystem besteht aus mehreren Stationen 1, die räumlich verteilt an unterschiedlichen geographischen Lokationen angeordnet sind. Eine solche Station wird auch als biometrischer Terminal 10 bezeichnet. Grundsätzlich sind die Station A, B, ... des Zugangskontrollsystems gleichartig aufgebaut. Jede der Stationen 1 hat einen Chipkartenleser 2 sowie einen Prozessor 3 und einen Sensor 4 für die Aufnahme eines biometrischen Merkmals. Die Sensoren 4 der Stationen 1 können dabei 15 identisch sein oder auch voneinander verschieden sein; insbesondere können die Sensoren 4 unterschiedlicher Stationen 1 von unterschiedlichen Herstellern stammen, ein unterschiedliches Auflösungsvcrmögen haben oder einen verschiedenen alterungsbedingten Zustand aufweisen.

[0044] Ferner hat jede Station 1 einen Speicherbereich 5 für die Speicherung einer Stationskennung sowie eine Ausgabeeinheit 6 für die Abgabe eines Freigabesignals bzw. für die Abgabe eines Signals zur Anzeige einer Zugangsverweigerung und/oder zur Anzeige weiterer Informationen für 25 den Benutzer.

[0045] Die autorisierten Benutzer des Systems haben jeweils eine Chipkarte 7. Jede der Chipkarten 7 ist also einem der Benutzer eindeutig zugeordnet. Die Chipkarte 7 beinhaltet einen Prozessor 8 sowie einen Speicherbereich 9 zur 30 Speicherung von biometrischen Referenz-Merkmals-Sätzen. Ein Prozessor 8 ist jedoch nicht unbedingt erforderlich; eine Implementierung der Erfindung ist auch möglich, wenn lediglich ein Speicher für die Speicherung von Merkmals-Sätzen vorhanden ist, wie das beispielsweise bei einem RF 35 ID Tag der Fall ist.

[0046] Diese Referenz-Merkmals-Sätze beziehen sich auf dasselbe biometrische Merkmal, wie zum Beispiel Gesichtsmerkmale, die Iris- oder Fingerabdruck-Merkmale des Benutzers. Die verschiedenen Referenz-Merkmals-Sätze in 40 dem Speicherbereich 9 sind jedoch voneinander verschieden, da sie unter verschiedenen Umgebungsbedingungen, wie zum Beispiel unterschiedlichen Beleuchtungsverhältnissen, und/oder für verschiedene Erscheinungsbilder des Benutzers und/oder mit verschiedenen Sensoren 4 aufgenommen worden sind. Jeder Referenz-Merkmals-Satz in 45 dem Speicherbereich 9 ist durch eine Merkmals-Satz-Kennung eindeutig identifiziert. Bei der Merkmals-Satz-Kennung kann es sich zum Beispiel um eine laufende Nummer des Referenz-Merkmals-Satzes handeln.

[0047] In einem Speicherbereich 10 der Chipkarte 7 ist eine Datei gespeichert, die jeder Merkmals-Satz-Kennung zumindest eine Stationskennung und eine Wertigkeit zuordnet. Die Stationskennung gibt dabei an, für welche Station oder für welche Stationen der Referenz-Merkmals-Satz mit 50 der betreffenden Merkmals-Satz-Kennung geeignet ist. Die Wertigkeit gibt eine Verifikationsgüte bei der Verwendung des betreffenden Referenz-Merkmals-Satzes bei einer bestimmten Station an. Die Wertigkeit ist also eine Maßzahl für die zu erwartende Übereinstimmung des Referenz-Merkmals-Satzes mit einem an der betreffenden Station zu 55 ermittelnden Verifikations-Merkmals-Satz.

[0048] Vorzugweise ist die Datei in dem Speicherbereich 10 so organisiert, dass jeder Stationskennung ein oder mehrere Tupel zugeordnet sind, wobei jedes der Tupel aus einer 60 Merkmals-Satz-Kennung und einer der Merkmals-Satz-Kennung zugeordneten Wertigkeit mit Bezug auf die betreffende Station besteht.

[0049] Die Chipkarte 7 beinhaltet ferner einen Speicher-

bereich 11 zur Speicherung einer Benutzerkennung sowie weitere personenbezogene Daten, wie zum Beispiel Name, Adresse und Telefonnummer, ein digitalisiertes Photo des Benutzers sowie Daten bezüglich der Zugangsrechte des Nutzers. Ferner beinhaltet die Chipkarte 7 einen Speicherbereich 12 zur Speicherung einer Aufnahme des biometrischen Merkmals des Benutzers in Form von Rohdaten oder eines aus einer solchen Aufnahme gewonnenen Verifikations-Merkmals-Satzes. In dem Speicherbereich 12 kann ferner die Stationskennung derjenigen Station abgespeichert werden, die die Aufnahme durchgeführt hat.

[0050] Wenn sich der Benutzer der Chipkarte 7 Zugang zu einem Bereich verschaffen möchte, der durch das Zugangskontrollsysteem geschützt ist, muss der Benutzer seine Chipkarte 7 in den Chipkartenleser 2 der betreffenden Station 1 einführen. Alternativ können auch berührungslos arbeitende Chipkarten 7 und Kartenleser 2 verwendet werden. Beispielsweise handelt es sich hierbei um die Station A. Vorzugsweise wird wie oben beschrieben vor der Benutzer-Authentisierung zunächst eine Chipkarten-Stations-Authentisierung vorgenommen. Zur Durchführung der Benutzer-Authentisierung wird dann automatisch zumindest ein Referenz-Merkmals-Satz aus dem Speicherbereich 9 ausgewählt, wobei die Stationskennung der Station A sowie die in dem Speicherbereich 10 gespeicherten Wertigkeiten berücksichtigt werden.

[0051] Mittels des Sensors 4 nimmt die Station A das biometrische Merkmal des Benutzers auf und erzeugt daraus durch ein entsprechendes Programm des Prozessors 3 einen Verifikations-Merkmals-Satz. Der Verifikations-Merkmals-Satz und der oder die ausgewählten Referenz-Merkmals-Sätze werden dann miteinander verglichen. Wenn mindestens einer der Referenz-Merkmals-Sätze hinreichend mit dem Verifikations-Merkmals-Satz übereinstimmt, gilt der Benutzer als authentisiert. Weitere Merkmalssätze brauchen dann nicht übertragen zu werden. Das Maß dieser Übereinstimmung ist die Verifikationsgüte, die mit einem entsprechenden Schwellwert verglichen wird. Vorzugsweise erfolgen die Vergleiche der ausgewählten Merkmals-Sätze mit dem Verifikations-Merkmals-Satz beginnend mit dem ausgewählten Merkmals-Satz der höchsten Wertigkeit, da hier die Wahrscheinlichkeit einer Übereinstimmung am höchsten ist. Danach folgen erforderlichenfalls weiterer Vergleiche mit weiteren ausgewählten Merkmals-Sätzen in der Reihenfolge absteigender Wertigkeiten.

[0052] Im Fall der Benutzer-Akzeptanz, d. h. wenn die Verifikationsgüte oberhalb des Schwellwerts liegt, wird ein entsprechendes Ausgabesignal über die Ausgabeeinheit 6 von der Station A abgegeben, so dass zum Beispiel eine Türverriegelung freigegeben wird.

[0053] Die Fig. 2 zeigt ein Diagramm zur Veranschaulichung einer Ausführungsform für die Durchführung des Authentisierungsverfahrens. Zu diesem Verfahren gehört ein Prozess 13, der auf der Chipkarte abläuft und ein Prozess 14, der stationsseitig abläuft.

[0054] Wenn die Chipkarte in den Chipkartenleser der Station eingeführt wird, sendet die Chipkarte in dem Schritt 15 die Benutzerkennung an die Station. Die Station prüft dann in dem Schritt 16, ob die Benutzerkennung zulässig ist, das heißt, ob sich der Benutzerkennung ein registrierter Benutzer zuordnen lässt und ob dieser Benutzer für den Zugang in den durch die Station gesicherten Gebäudeteil autorisiert ist. Wenn dies der Fall ist, wird von der Station eine Nutzerbestätigung an die Chipkarte ausgegeben.

[0055] Die Chipkarte sendet daraufhin in dem Schritt 17 eine Merkmalsliste von Referenz-Merkmals-Sätzen an die Station. Bei dieser Merkmalsliste handelt es sich vorzugsweise um die in dem Speicherbereich 10 (vgl. Fig. 1) ge-

speicherte Datei, bestehend aus den Merkmals-Satz-Kennungen und den zugeordneten Stationskennungen und Wertigkeiten. Eine Übertragung von Referenz-Merkmals-Sätzen selbst ist also noch nicht erforderlich.

- 5 [0056] In dem Schritt 18 ermittelt die Station aus der Merkmalsliste einen oder mehrere Referenz-Merkmals-Sätze. Die Auswahl des oder der Referenz-Merkmals-Sätze aus der Liste erfolgt dabei basierend auf der Stationskennung der betreffenden Station, vorzugsweise unter Berücksichtigung der Wertigkeiten.
- 10 [0057] Beispielsweise werden aus der Merkmalsliste zunächst diejenigen Merkmals-Satz-Kennungen ermittelt, denen die Stationskennung der betreffenden Station zugeordnet ist. Aus der Menge dieser Merkmals-Satz-Kennungen mit der Stationskennung kann dann wiederum eine Auswahl basierend auf den Wertigkeiten erfolgen.
- 15 [0058] In dem Schritt 19 fordert die Station von der Chipkarte den oder die ausgewählten Referenz-Merkmals-Sätze an, indem die betreffende Merkmals-Satz-Kennung bzw. die 20 Merkmals-Satz-Kennungen an die Chipkarte übertragen werden.
- 25 [0059] In dem Schritt 20 beginnt die Chipkarte dann die ausgewählten Referenz-Merkmals-Sätze aus dem entsprechenden Speicherbereich (vgl. Speicherbereich 9 der Chipkarte 7 in Fig. 1) auszulesen und an die Station zu übertragen. Dies erfolgt vorzugsweise beginnend mit dem ausgewählten Referenz-Merkmals-Satz der höchsten Wertigkeit. Für den Fall, dass mehrere Referenz-Merkmals-Sätze zu übertragen sind, werden diese vorzugsweise sequentiell sortiert nach abnehmender Wertigkeit übertragen, das heißt die Übertragung des ausgewählten Referenz-Merkmals-Satzes mit der höchsten Wertigkeit erfolgt zuerst.
- 30 [0060] Bevorzugt wird von der Station schon vor oder während der Übertragung des oder der Referenz-Merkmals-Sätze von der Chipkarte in dem Schritt 21 das biometrische Merkmal des Benutzers mittels des Biometriesensors der Station aufgenommen. Daraus wird in dem Schritt 2 ein Verifikations-Merkmals-Satz extrahiert.
- 35 [0061] In dem Schritt 23 wird dann der Verifikations-Merkmals-Satz mit dem Referenz-Merkmals-Satz der höchsten Wertigkeit verglichen. Falls keine hinreichende Übereinstimmung zwischen dem Verifikations-Merkmals-Satz und dem Referenz-Merkmals-Satz festgestellt werden kann, werden gegebenenfalls weitere Vergleiche mit den weiteren 40 Referenz-Merkmals-Sätzen geringerer Wertigkeit durchgeführt.
- 45 [0062] Falls zwischen einem der Referenz-Merkmals-Sätze und dem Verifikations-Merkmals-Satz eine hinreichende Übereinstimmung festgestellt werden kann, wird in dem Schritt 24 geprüft, ob dem Referenz-Merkmals-Satz, der zu der Freigabe geführt hat, eine entsprechende Wertigkeit zugeordnet ist.
- 50 [0063] Eine Möglichkeit für die Adaption der Wertigkeiten ist die folgende: Wenn die dem Freigabe-Referenz-Merkmals-Satz zugeordnete Wertigkeit wesentlich geringer ist als die tatsächlich erreichte Verifikationsgüte, so wird diese Wertigkeit entsprechend angepasst und an die Chipkarte übertragen. Auf der Chipkarte wird dann die 55 ursprünglich in der Datei in dem Speicherbereich 10 (vgl. Fig. 1) gespeicherte Wertigkeit durch die angepasste Wertigkeit überschrieben. Dies erfolgt in dem Schritt 25. Entsprechend können die anderen Wertigkeiten des ausgewählten Merkmals-Sätze angepasst werden.
- 60 [0064] Falls sich herausstellt, dass zwischen keinem der Referenz-Merkmals-Sätze und dem Verifikations-Merkmals-Satz eine hinreichende Übereinstimmung besteht, wird in dem Schritt 25 durch die Station die in dem Schritt 21 gefertigte Aufnahme an die Chipkarte übertragen. Dies kann

beispielsweise in Form von-Rohdaten erfolgen.

[0065] Alternativ kann auch der in dem Schritt 2 aus der Aufnahme gewonnene Verifikations-Datensatz an die Chipkarte übertragen werden. In dem Schritt 27 wird die Aufnahme bzw. der Verifikations-Merkmales-Satz der Aufnahme in dem betreffenden Speicherbereich (vgl. Speicherbereich 12 der Chipkarte 7 in Fig. 1) abgelegt.

[0066] Ferner erhält der Benutzer von der Station die Aufforderung, sich an seinen Administrator zu wenden. Der Administrator hat dann die Möglichkeit in dem Schritt 28 auf die gespeicherte Aufnahme zuzugreifen, um hieraus einen neuen Referenz-Merkmales-Satz zu generieren. Alternativ schaltet der Administrator den zuvor chipkartenseitig gespeicherten Verifikations-Merkmales-Satz als neuen Referenz-Merkmales-Satz frei.

[0067] Die Fig. 3 zeigt eine alternative Ausführungsform, bei der die Auswahl der Referenz-Merkmales-Sätze chipkartenseitig erfolgt und der Vergleich stationssseitig. Chipkartenseitig läuft dabei der Prozess 29 und stationsseitig der Prozess 30 ab.

[0068] In dem Schritt 31 sendet die Chipkarte wiederum die Benutzerkennung. In dem Schritt 32 wird stationsseitig die Zulässigkeit der Benutzerkennung geprüft. Dies entspricht den Schritten 15 und 16 der Fig. 2. Im Unterschied zu der Ausführungsform der Fig. 2 wird für den Fall, dass die Benutzerkennung zulässig ist, neben der Nutzerbestätigung auch die Stationskennung mit zu der Chipkarte übertragen.

[0069] Diese ermittelt dann in dem Schritt 33 einen oder mehrere Referenz-Merkmales-Sätze für die BenutzerAuthentisierung. Dies entspricht dem Schritt 18 der Fig. 2, wobei in der Ausführungsform der Fig. 3 diese Auswahl von der Chipkarte und nicht von der Station getroffen wird. Der oder die ausgewählten Referenz-Merkmales-Sätze werden dann zu der Station übertragen. Die nachfolgenden Schritte 34 bis 41 entsprechen den Schritten 21 bis 28 der Fig. 2.

[0070] In der Ausführungsform der Fig. 4 erfolgt sowohl die Auswahl des oder der Referenz-Merkmales-Sätze als auch der Vergleich chipkartenseitig. Hierzu laufen die Prozesse 42 chipkartenseitig und 43 stationsseitig ab. Die Schritte 44, 45 und 46 der Ausführungsform der Fig. 4 entsprechen den Schritten 31, 32 und 33 der Ausführungsform der Fig. 3. Ferner entsprechen die Schritte 47 und 48 hinsichtlich der Ermittlung des Verifikations-Merkmales-Satzes den Schritten 34 und 35 der Ausführungsform der Fig. 3.

[0071] Im Unterschied zu der Ausführungsform der Fig. 2 und 3 wird keiner der ausgewählten Referenz-Merkmales-Sätze von der Chipkarte an die Station übertragen, sondern der Vergleich findet auf der Chipkarte selbst in dem Schritt 49 statt.

[0072] Der Schritt 50 entspricht dem Schritt 37 der Ausführungsform der Fig. 3, mit dem Unterschied, dass dieser Schritt von der Chipkarte selbst ausgeführt wird. Der Schritt 51 entspricht dem Schritt 39 der Ausführungsform der Fig. 3, wobei auch dieser Schritt von der Chipkarte selbst ausgeführt wird und die Chipkarte von der Station die Aufnahme bzw. den Verifikations-Merkmales-Satz erforderlichenfalls anfordert, um die Aufnahme bzw. den Verifikations-Merkmales-Satz abzuspeichern. Die Schritte 52 und 53 entsprechen dann wiederum den Schritten 40 und 41 der Ausführungsform der Fig. 3.

Bezugszeichenliste

- 1 Station
- 2 Chipkartenleser
- 3 Prozessor
- 4 Sensor

- 5 Speicherbereich
- 6 Ausgabeeinheit
- 7 Chipkarte
- 8 Prozessor
- 9 Speicherbereich
- 10 Speicherbereich
- 11 Speicherbereich
- 12 Speicherbereich
- 13 Prozess
- 14 Prozess

Patentansprüche

1. Datenträger für die biometrische Benutzer-Authentisierung mit Mitteln zur Speicherung von zumindest einem ersten biometrischen Merkmals-Satz (9, 10) und einem zweiten biometrischen Merkmals-Satz (9, 10), wobei die ersten und zweiten biometrischen Merkmals-Sätze voneinander verschieden sind, zu dem selben Benutzer gehören und dasselbe biometrische Merkmal betreffen.
2. Datenträger nach Anspruch 1, wobei dem ersten und dem zweiten biometrischen Merkmals-Satz je ein oder mehreren Stationen (1) zugeordnet sind.
3. Datenträger nach Anspruch 1 oder 2, wobei dem ersten und dem zweiten biometrischen Merkmals-Satz je zumindest eine Wertigkeit betreffend eine Verifikationsgüte zugeordnet ist.
4. Datenträger nach Anspruch 1, 2 oder 3, wobei der dem ersten und dem zweiten biometrischen Merkmals-Satz je eine oder mehrere Stationen (1) zugeordnet sind und jeder Zuordnung einer Station zu einem der Merkmals-Sätze eine Wertigkeit betreffend eine Verifikationsgüte zugeordnet ist.
5. Datenträger nach einem der vorhergehenden Ansprüche 1 bis 4 mit Mitteln zum Empfang einer Stationskennung und mit Prozessormitteln (8) zur Auswahl eines Merkmals-Satzes aus den zumindest ersten und zweiten Merkmals-Sätzen basierend auf der Stationskennung.
6. Chipkarte nach Anspruch 5, bei der die Prozessormittel so ausgebildet sind, dass zur Auswahl des Merkmals-Satzes auf die Zuordnung von Stationen zu den zumindest ersten und zweiten Merkmals-Sätzen und vorzugsweise auf die jeweiligen Wertigkeiten zugegriffen wird.
7. Datenträger nach Anspruch 5 oder 6, bei der die Prozessormittel so ausgebildet sind, dass aus den zumindest ersten und zweiten Merkmals-Sätzen, denen eine Station mit der empfangenen Stationskennung zugeordnet ist, derjenige Merkmals-Satz ausgewählt wird, dem die höchste Wertigkeit mit Bezug auf diese Station zugeordnet ist.
8. Datenträger nach einem der vorhergehenden Ansprüche 1 bis 7 mit Mitteln zum Empfang eines Merkmals-Satzes von einer Station und mit Prozessormitteln (8) zum Vergleich des empfangenen Merkmals-Satzes mit einem aus den zumindest ersten und zweiten Merkmals-Sätzen ausgewählten Merkmals-Satz.
9. Datenträger nach einem der vorhergehenden Ansprüche 1 bis 9 mit Mitteln (8) zur Anpassung der Wertigkeit in Abhängigkeit von dem Ergebnis des Vergleichs eines von der Station empfangenen Merkmals-Satzes mit dem ersten oder zweiten Merkmals-Satz, wobei die Wertigkeit zugewandt ist.
10. Datenträger nach einem der vorhergehenden Ansprüche 1 bis 9 mit Mitteln zur Speicherung einer Aufnahme des biometrischen Merkmals.

11. Station für die biometrische Benutzer-Authentisierung mit Mitteln (4) zur Aufnahme eines biometrischen Merkmals, Mitteln (2) zum Empfang von Daten betreffend zumindest einen ersten biometrischen Merkmals-Satz und einen zweiten biometrischen Merkmals-Satz, wobei die ersten und zweiten Merkmals-Sätze voneinander verschieden sind, zu dem selben Benutzer gehören und dasselbe biometrische Merkmal betreffen. 5

12. Station nach Anspruch 11 mit Mitteln zum Senden einer Stationskennung (5) an den Datenträger. 10

13. Station nach Anspruch 11 oder 12 mit Prozessormitteln (3) zur Auswahl eines Merkmals-Satzes aus zumindest den ersten und zweiten Merkmals-Sätzen. 15

14. Station nach Anspruch 11, 12 oder 13, bei der die Prozessormittel so ausgebildet sind, dass zur Auswahl des Merkmals-Satzes auf die Zuordnung von Stationen zu den zumindest ersten und zweiten Merkmals-Sätzen und vorzugsweise auf die jeweiligen Wertigkeiten zugegriffen wird. 20

15. Station nach einem der vorhergehenden Ansprüche 11 bis 14, bei der die Prozessormittel so ausgebildet sind, dass aus den zumindest ersten und zweiten Merkmals-Sätzen, denen die Station zugeordnet ist, 25 derjenige Merkmals-Satz ausgewählt wird, der die höchste Wertigkeit mit Bezug auf diese Station hat.

16. Station nach einem der vorhergehenden Ansprüche 11 bis 15, mit Mitteln (2) zum Erzeugung eines Verifikations-Merkmals-Satzes und mit Prozessormitteln (8) zum Vergleich des Verifikations-Merkmals-Satzes mit einem aus den zumindest ersten und zweiten Merkmals-Sätzen ausgewählten Merkmals-Satz. 30

17. Station nach einem der vorhergehenden Ansprüche 11 bis 16, mit Mitteln (3) zur Anpassung der Wertigkeit in Abhängigkeit von dem Ergebnis des Vergleichs eines Verifikations-Merkmals-Satzes mit dem ersten oder zweiten Merkmals-Satz, welchem die Wertigkeit zugeordnet ist. 35

18. Station nach einem der vorhergehenden Ansprüche 11 bis 17 mit Mitteln zur Sendung der Aufnahme an den Datenträger, wenn die Benutzer-Authentisierung fehlgeschlagen ist. 40

19. System für die biometrische Benutzer-Authentisierung mit zumindest einem Datenträger nach einem der vorhergehenden Ansprüche 1 bis 10 und mit zumindest einer Station nach einem der vorhergehenden Ansprüche 11 bis 18. 45

20. Verfahren für die biometrische Benutzer-Authentifizierung mit folgenden Schritten: 50

- Auswahl eines Merkmals-Satzes aus einem ersten biometrischen Merkmals-Satz und einem zweiten biometrischen Merkmals-Satz, wobei die ersten und zweiten Merkmals-Sätze voneinander verschieden sind, zu dem selben Benutzer gehören und dasselbe biometrische Merkmal betreffen, 55
- Aufnahme des biometrischen Merkmals,
- Generierung eines Verifikations-Merkmals-Satzes aus der Aufnahme,
- Vergleich des ausgewählten Merkmals-Satzes mit den Verifikations-Merkmals-Satz für die Durchführung der Benutzer-Authentisierung. 60

21. Verfahren nach Anspruch 20, wobei die Auswahl des Merkmals-Satzes aus den zumindest ersten und zweiten Merkmals-Sätzen basierend auf einer Stationskennung erfolgt. 65

22. Verfahren nach Anspruch 20 oder 21, wobei die Auswahl des Merkmals-Satzes aus den zumindest er-

sten und zweiten Merkmals-Sätzen basierend auf einer Wertigkeit betreffend eine Verifikationsgüte erfolgt. 23. Verfahren nach Anspruch 22, wobei eine Anpassung der Wertigkeit erfolgt, wenn die tatsächliche Verifikationsgüte nicht der Wertigkeit entspricht. 24. Verfahren nach einem der vorhergehenden Ansprüche 20 bis 23, wobei die Aufnahme des biometrischen Merkmals auf einem Datenträger gespeichert wird. 25. Verfahren nach einem der vorhergehenden Ansprüche 20 bis 24, wobei der Verifikations-Merkmals-Satz auf dem Datenträger gespeichert wird, wenn die Benutzer-Authentisierung fehlgeschlagen ist. 26. Computerprogrammprodukt zur Durchführung eines Verfahrens nach einem der vorhergehenden Ansprüche 20 bis 25.

Hierzu 4 Scite(n) Zeichnungen

- Leerseite -

THIS PAGE BLANK (USPTO)

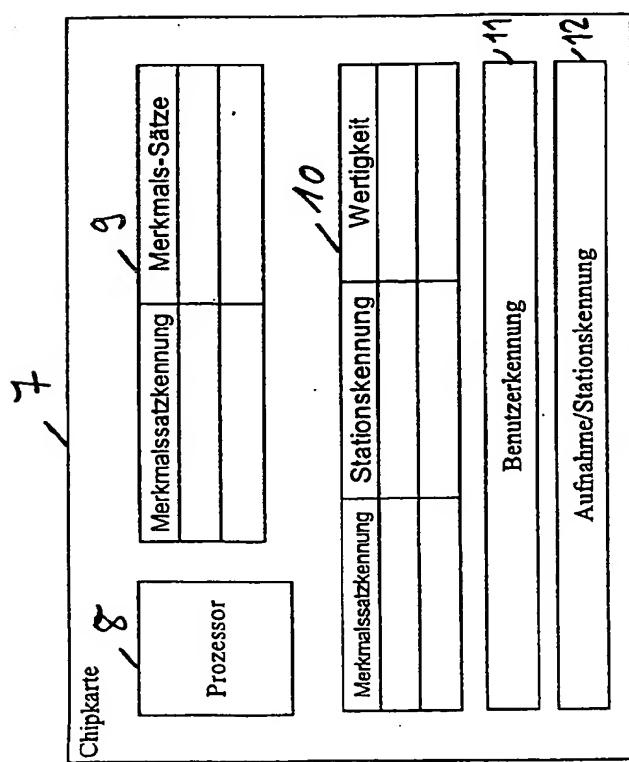
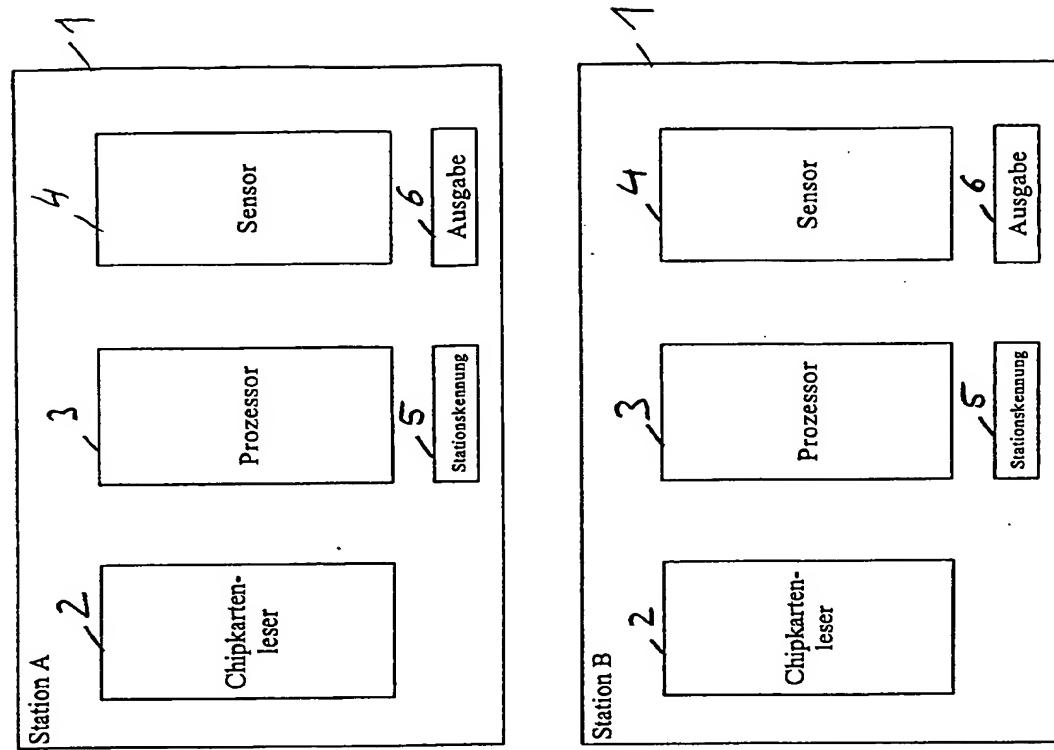


Fig. 1

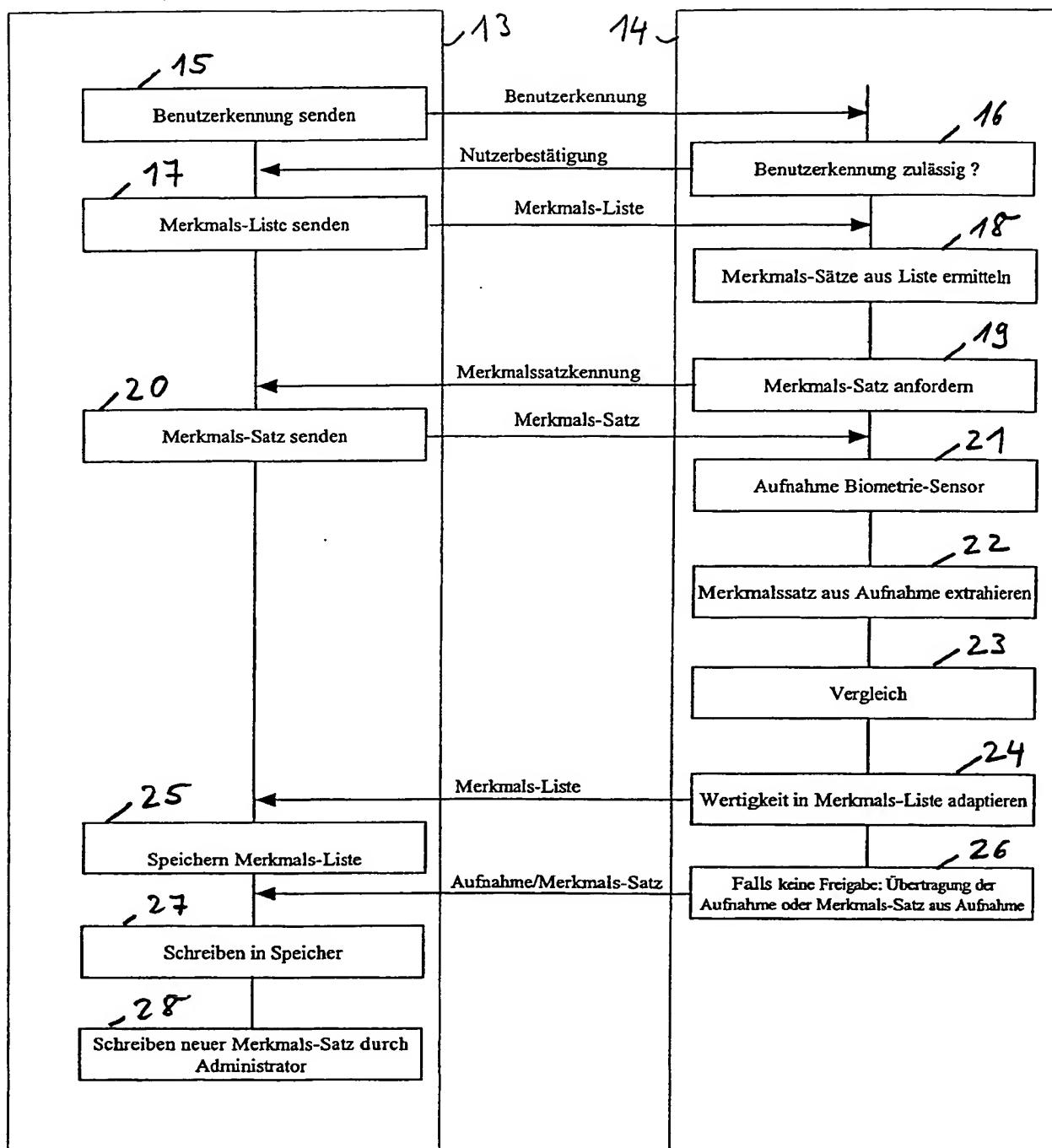


Fig. 2

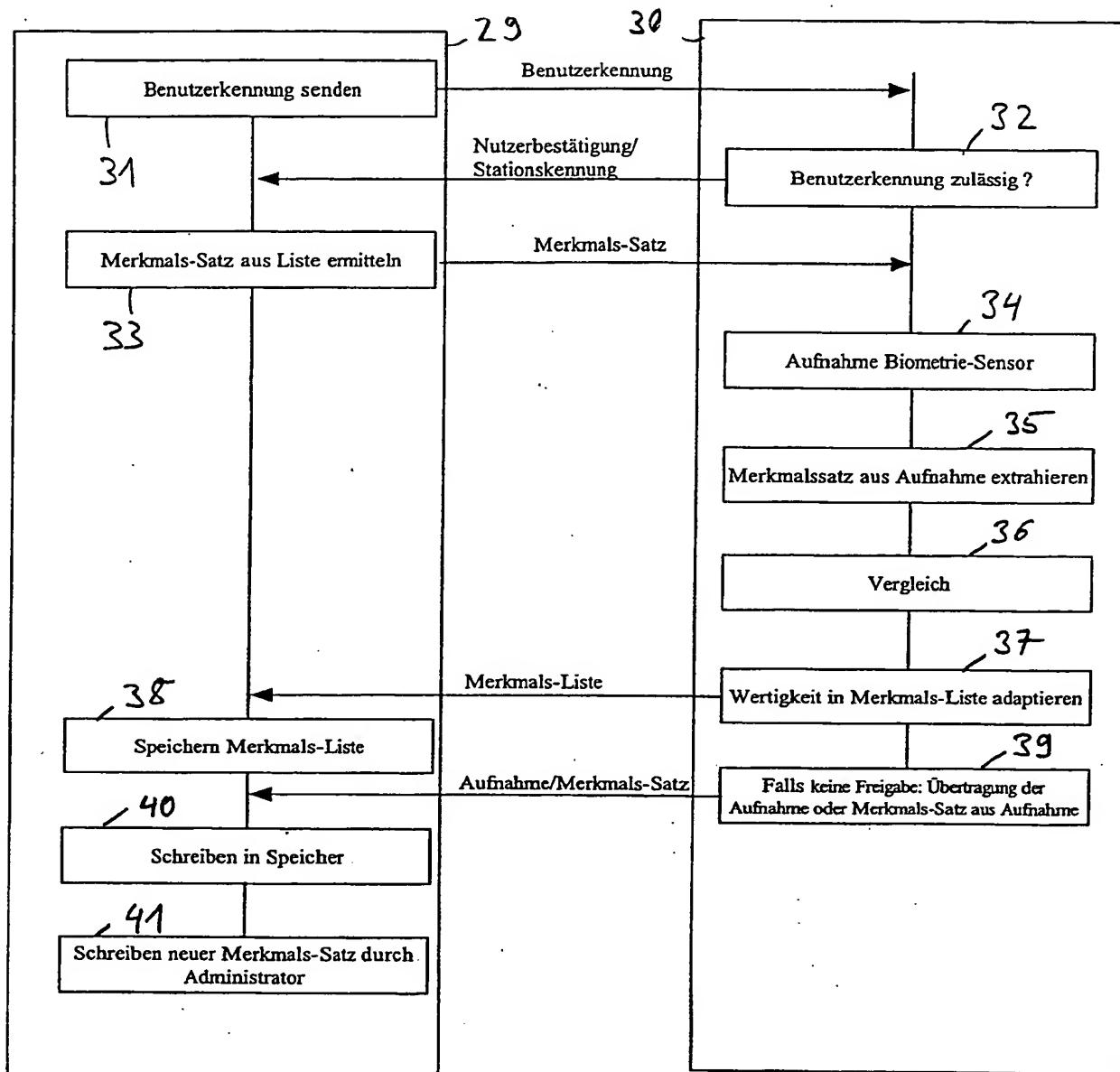


Fig. 3

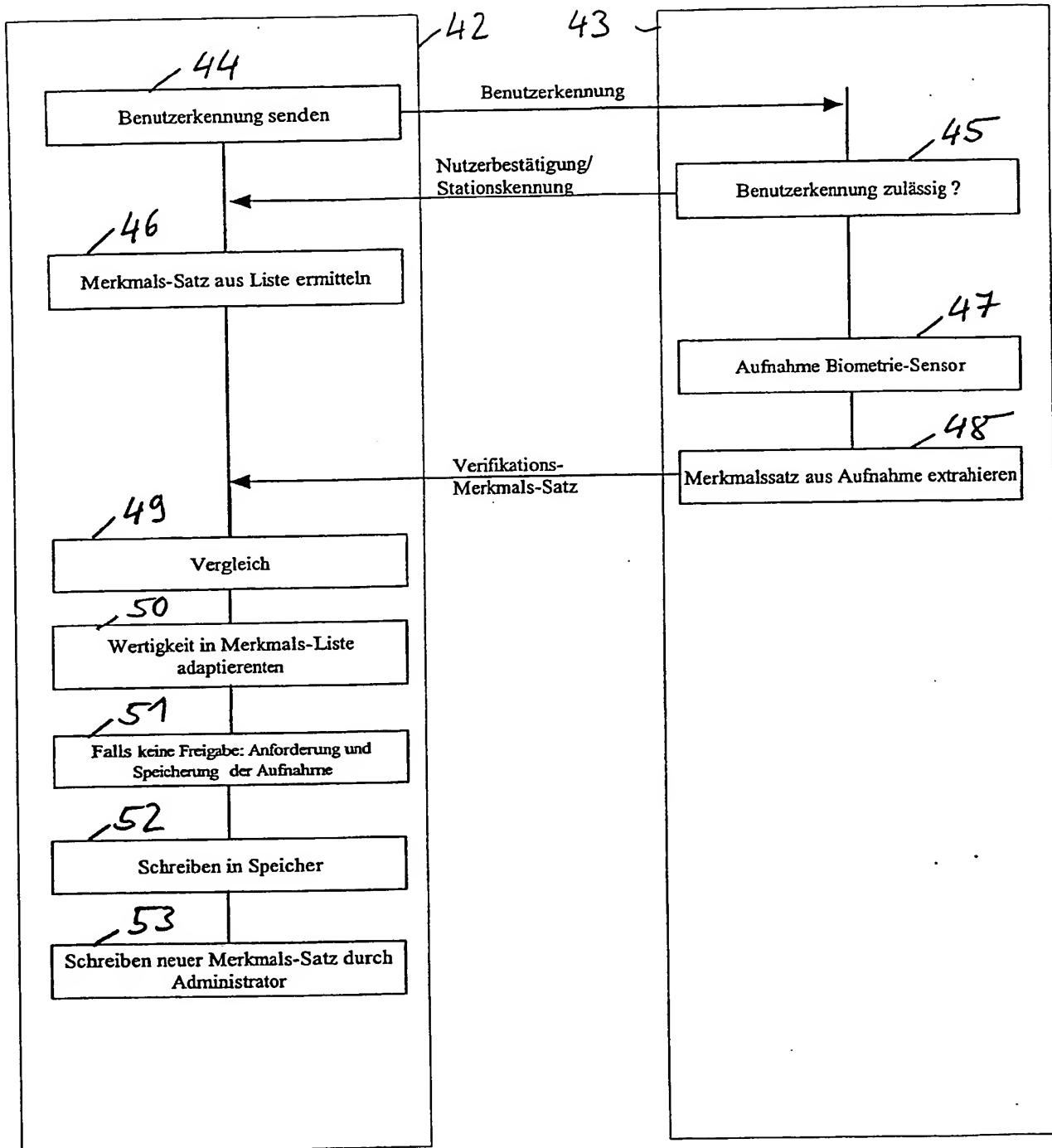


Fig. 4